Date of publication SEP-30, 2025, date of current version AUG-19, 2025.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.19.3.XX

Analysis of the Impact of Encryption on the Traffic Volumes of IoT Protocols

VIKTOR KOZEL, OLEKSII IVANCHUK, IEVGENIIA DROZDOVA, OLENA PRYKHODKO
[1]Kherson National Technical University, Kherson, Ukraine

Corresponding author: Viktor Kozel (e-mail: k_vic@ukr.net).

ABSTRACT The article discusses the problem of increasing traffic volumes due to the availability of encryption. Data packets of the Wi-Fi, Bluetooth, 6LoWPAN standards, and the ZigBee, WirelessHART, and NB-IoT protocols were considered for testing the impact. Based on information about the data packets, it was determined which parts of the packet were to be encrypted and by what algorithm. Since there is an impact on the volume of the data packets, its study was carried out. For this purpose, graphs of the dependence of the volume of additions on the payload volume were built. The resulting graphs have a sawtooth shape because the addition will be the maximum possible size at a specific payload size. It was concluded that the Wi-Fi standard is the best in conditions without restrictions on the payload size, and NB-IoT is the worst. In conditions of the limited size of the payload, ZigBee is the best, and NB-IoT is the worst.

KEYWORDS Internet of Things, Wi-Fi, Bluetooth, ZigBee, WirelessHART, 6LoWPAN, NB-IoT, AES, Data packet size, Encryption.

I. INTRODUCTION

The distribution of new IoT devices creates an increased load on the transmission environment in which they operate. If data transmission protocols use encryption, a packet's amount of data transmitted may be affected. Therefore, it is necessary to analyze the data packets of IoT protocols and standards to determine the level of impact and choose the optimal protocol or standard that will have the least impact.

This material continues the IoT protocols and standards analysis conducted in [1]. It described the automation of the protocol selection process when building IoT systems using software that asks the user for the parameters of the resulting system and selects the optimal protocols recommended for use in the system. The study of the impact of encryption will improve the selection process by adding an indicator, which can be decisive if several protocols are equal in capabilities and meet the requirements.

II. RELATED LITERATURE

In works [2,3], an analysis of existing optimization methods in Internet of Things protocols and their impact on energy consumption during data transmission was conducted. Still, an analysis of the effect of encryption on traffic volumes and overall energy consumption was not performed.

The paper [4] considers the impact of encryption on the size of media data packets. However, the Internet of Things has different protocols and standards, so it is impossible to assess the impact of encryption on them based only on the data from [4].

The paper [5] examines encryption in microcontrollers used to develop IoT devices. The results show that encryption impacts data processing time, but the study does not consider potential delays in transmitting encrypted data.

III. MATERIALS AND METHODS

The following standards and protocols are most commonly used for the Internet of Things: Wi-Fi, Bluetooth, ZigBee, WirelessHART, 6LoWPAN, and NB-IoT.

In each of the presented protocols, the amount of payload per packet is not fixed and may be less than what the protocol or standard specifies. Therefore, for each protocol, it was determined which parts of the packet were to be encrypted and whether additional payloads were required for successful encryption.

The Wi-Fi standard is used to organize a wireless local

area network. The network uses radio waves in the 900 MHz, 2.4 GHz, or 5 GHz frequency band according to the IEEE 802.11 standard [6]. The topology used is a star, which implies the presence of a central network coordinator (router) to which all devices are connected. Usually, smartphones, tablets, laptops, and SMART TVs access the Internet via Wi-Fi. With the distribution of IoT systems, Wi-Fi networks have also been used to connect IoT devices to the global network, allowing them to receive information and control these devices from anywhere with a worldwide network connection.

All devices connected to a Wi-Fi network use the same frequency range, which often causes errors from simultaneous data transmission by several devices. This problem is solved by searching for simultaneous transmission collisions in the network - CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) [7]. When new devices are added to the network, the data transmitted increases. An analysis of the standard's encryption method will help determine whether it significantly impacts the traffic volume of a single device, which will block the transmission medium for a long time.

The structure of a Wi-Fi data packet is shown in Figure 1 [8].

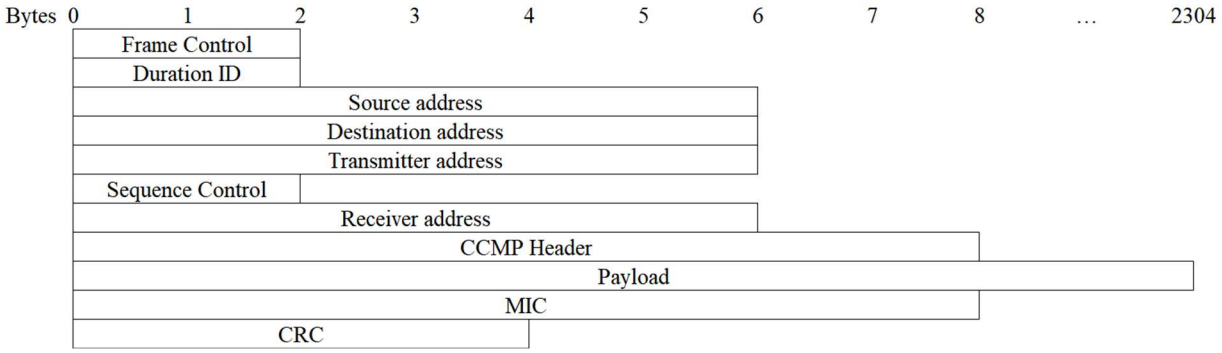

Figure 1. The structure of a Wi-Fi data packet

The primary attention should be paid to the packet's CCMP Header, Payload, and MIC parts involved in data encryption. The AES algorithm encrypts the payload with the CCMP protocol [9,10,11]. The MIC part is a code calculated as a checksum of the payload in the packet and enables checking the correctness of data transmission. The Payload and MIC parts are encrypted as a whole.

The AES algorithm has several encryption options. The AES-CTR version with a 128-bit (16-byte) key encrypts data on Wi-Fi. According to it, the algorithm is fed with a counter that has increased since the start. Unique counter values are used for each payload block, reducing the risk of unauthorized persons' decryption. At the beginning of the encryption process, the payload must be supplemented to a size that is a multiple of the key size, corresponding to 128 bits.

The initial data can be supplemented with up to 127 bits, negatively impacting the data transmitted. The amount of data received after the addition does not change during encryption. The second addition to the data packet size is the CCMP header. It contains the data packet number, a blank byte reserved for future use, and an encryption parameter byte. In this byte, bit 5 is always set to 1 to indicate that AES encryption is used.

Bytes 6-7 store the key identifier used for encryption if keys have been predefined. Bytes 0-4 are reserved for the future. This means that one byte is added to perform encryption, and the total size of the data packet increases from 1 to 127 bits, depending on the amount of addition to the original data. The payload may be smaller for small volumes than the additional information required for encryption.

The Bluetooth standard exchanges data over short distances (up to 10 meters) [12]. Bluetooth became the Internet of Things standard when it received an energy-efficient version of Bluetooth LE [13]. It uses a 2.4 GHz radio channel for data exchange. Like Wi-Fi, the standard uses a star topology for its operation. The standard has the same problem with collisions and uses CSMA/CA to find them.

The structure of a Bluetooth data packet is shown in Figure 2.

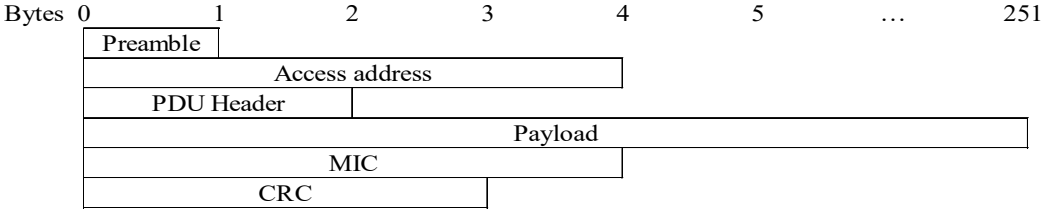

Figure 2. The structure of a Bluetooth data packet

The Bluetooth standard has two main parts involved in encryption - the Payload and MIC. Bluetooth has an encryption algorithm similar to Wi-Fi. It uses the AES encryption method in the AES-CTR version with a 128-bit key [14]. The Payload part is responsible for the payload, and the MIC is responsible for the checksum to verify the integrity of the payload. During encryption, the Payload and MIC are combined and encrypted as one. Since the AES algorithm requires the data length to be a multiple of the encryption key (128 bits), the combined data is multiplied. Unlike Wi-Fi, the Bluetooth standard does not have an additional byte with encryption parameters, so the maximum increase in packet size can be up to 127 bits.

The ZigBee protocol was created to implement a "smart home" based on the IEEE 802.15.4 standard [15]. The protocol has 3 radio frequency bands for operation: 866 MHz in Europe, 915 MHz in the USA and Australia, and 2.4 GHz in other countries [16]. The ZigBee network is built on a mesh topology, enabling network devices to route traffic until it reaches the network coordinator freely.

The structure of a data packet is shown in Figure 3.

The packet's APS Header, ZCL Header, and Payload parts are encrypted. The Payload part stores the payload transmitted in the packet. The APS Header controls communication with the cluster to which the transmitting device belongs. The ZCL Header determines the direction of the packet transmission between the client and the server and the type of command to be transmitted.

The AES algorithm is also used in the AES-CTR version with a 128-bit encryption key [17]. Since it is necessary to ensure the key multiplicity, adding up to 127 bits to the data packet is needed, which affects the traffic volume.

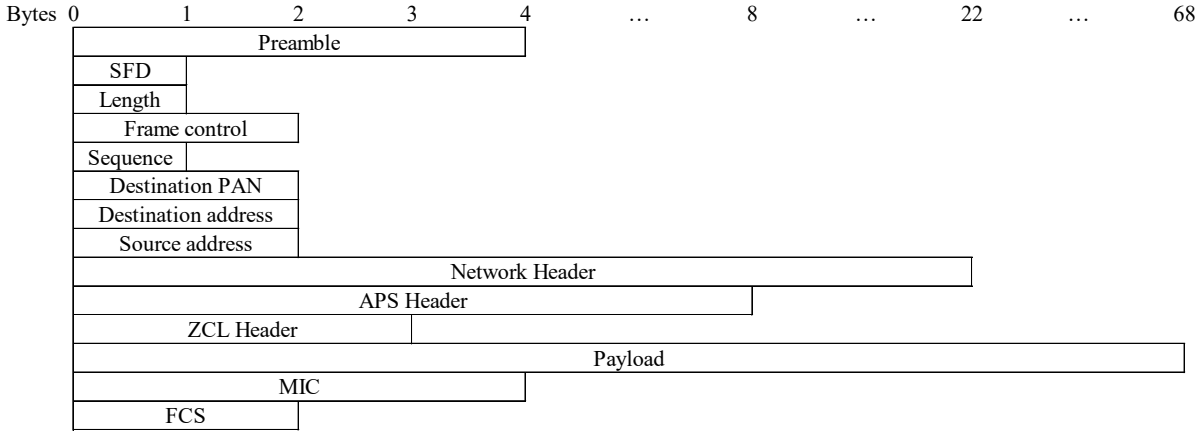

Figure 3. The structure of a ZigBee data packet

The MIC part is encrypted separately using the AES algorithm in the AES-CBC version. After encryption, only a portion of the upper 4 bytes remains unencrypted. Since the size of the MIC part is fixed, it does not affect the size of the data packet.

The 6LoWPAN standard was also created specifically for the Internet of Things. It is also based on the IEEE 802.15.4 standard for operation at the lower layers of the OSI standard [18]. It uses a 2.4 GHz mesh network as a topology. The main difference between ZigBee and ZigBee is the use of IPv6 addressing. The packet structure is shown in Figure 4 [19].

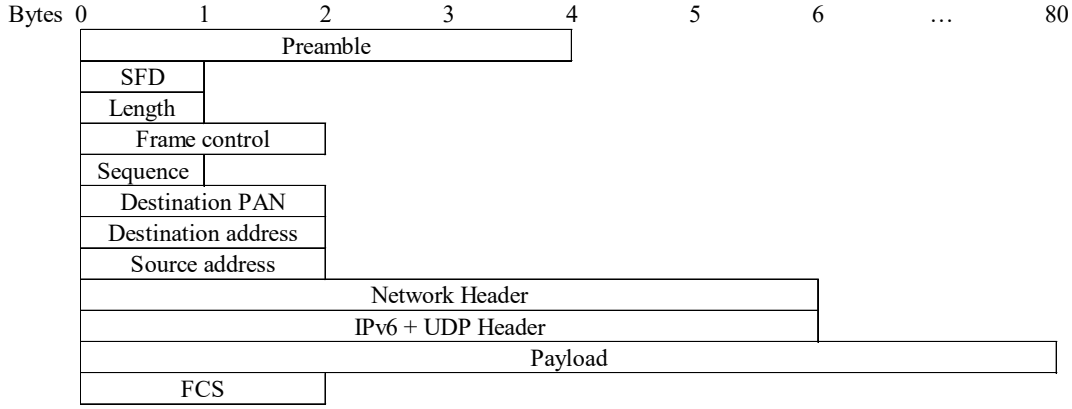

Figure 4. The structure of a 6LoWPAN data packet

The IPv6+UDP Header and Payload parts are encrypted in the data packet. The Payload part is responsible for the payload. The IPv6+UDP Header stores IPv6 addressing data and UDP data headers.

The encryption is based on the AES algorithm in the AES-CTR version with a key size of 128 bits [19,20]. During encryption, these parts are combined into a single text and encrypted together. The encryption requires an addition of 1 to 127 bits, which affects the amount of data in the packet.

The WirelessHART protocol is more similar to ZigBee than 6LoWPAN. It is also based on the IEEE 802.15.4 standard [21, 22, 23]. Figure 5 shows a data packet of the protocol.

The Security Header and Payload parts are encrypted in the data packet. The encryption is based on the AES algorithm in the AES-CBC version [24]. The algorithm requires data to be supplemented with a key size of 128 bits. Because of this, the amount of the addition can range from 1 to 127 bits, increasing the packet size.

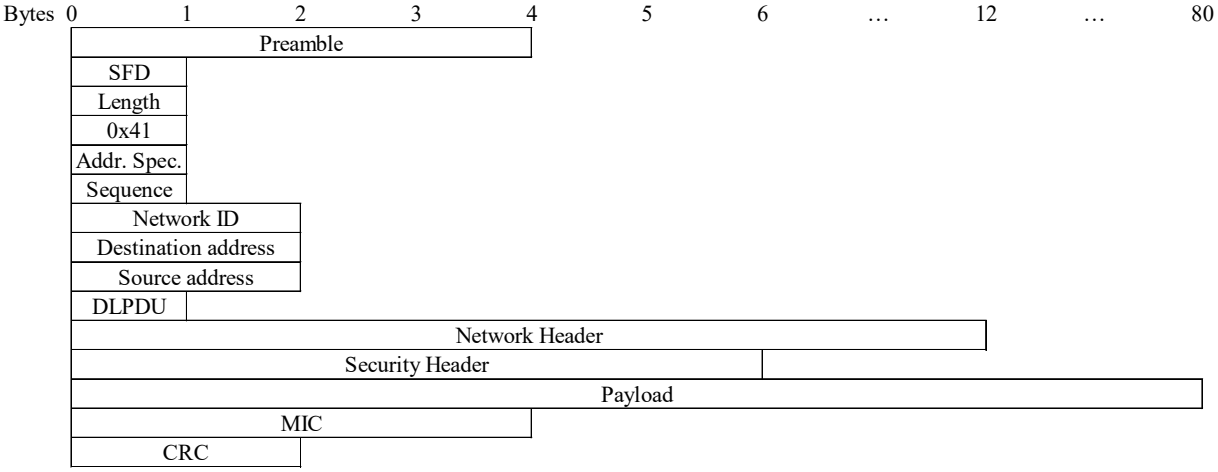

Figure 5. The structure of a WirelessHART data packet

NB-IoT is an Internet of Things protocol that uses a cellular network at a radio frequency of 800, 900, or 1800 MHz to connect devices up to several kilometers away [25]. Most of the protocol specifications are borrowed from the LTE protocol, which allows the system to be deployed on existing cellular network equipment.

Figure 6 shows the structure of an NB-IoT data packet.

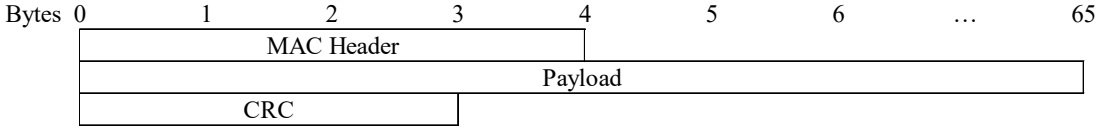

Figure 6. The structure of a NB-IoT data packet

During data transmission, the Payload part is encrypted. The ESP protocol, based on the 128-EEA2 algorithm [26,27], is used for encryption. This algorithm involves adding the payload to a key size of 128 bits. As a result, the amount of encrypted data can increase from 1 to 127 bits.

In each of the presented protocols, there is a problem of increasing the transmitted packet due to data encryption, which requires supplementing the payload with additional bits to the key size.

Since the negative impact of additions is evident, it is necessary to calculate the volume of additions in each protocol for all possible payload volumes. The following formula was used for the calculation:

$$a = (b - ((x + c) \ mod \ b)) \ mod \ b, \quad (1)$$

where a is the volume of addition to the size of the encryption block in bits, c is the amount of data encrypted together with the payload in bits (Table 1), b is the size of the encryption key in bits, and x is the volume of payload in bits.

In some protocols, parts of the data packet are encrypted together with the payload, so the size of these blocks must be considered when calculating the addition of the key size. Table 1 shows these blocks and their size in bits.

Table 1. Sizes of permanent blocks of data packets encrypted together with the payload

Protocol or standard	Blocks of data packets	Sizes
Wi-Fi	CCMP Header and MIC	128 bits

Bluetooth	MIC	32 bits
6LoWPAN	APS Header and ZCL Header	88 bits
WirelessHART	IPv6+UDP Header	48 bits
ZigBee	Security Header	48 bits
NB-IoT	-	0 bits

To evaluate the impact of additions on the size of the data packet, the percentage of additions relative to the size of the encrypted data was calculated using Formula 2.

$$y = \frac{a}{a+x} \times 100\%, \quad (2)$$

Using the formula (2), the graphs were built showing how the volume of additions depends on the volume of payload in the total encrypted data (Figs. 7-12). The axis of abscissa is limited to the maximum amount of payload that a Wi-Fi protocol can transmit in one package. All other protocols can transmit a smaller payload, limiting their graphics. This restriction was chosen to allow the possibility of superimposing graphs to compare them.

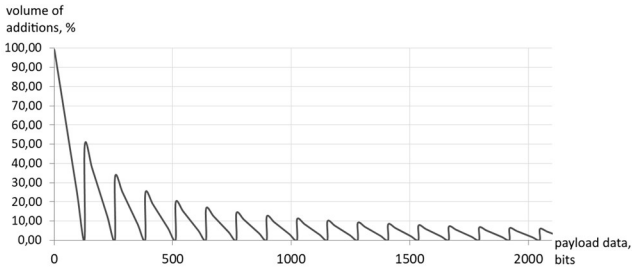

Figure 7. The volume of additions in the Wi-Fi standard

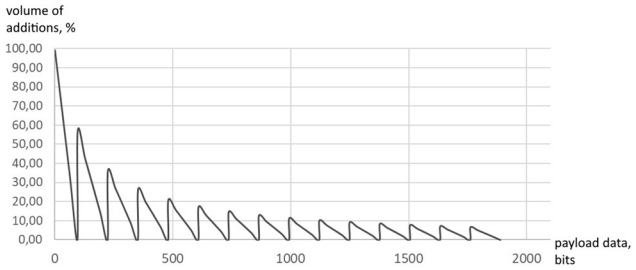

Figure 8. The volume of additions in the Bluetooth standard

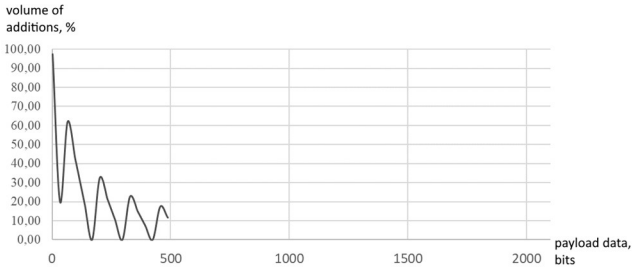

Figure 9. The volume of additions in the ZigBee protocol

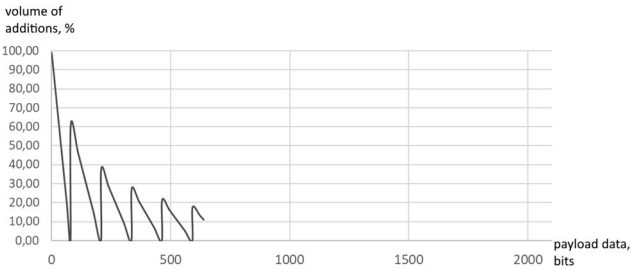

Figure 10. The volume of additions in the 6LoWPAN standard

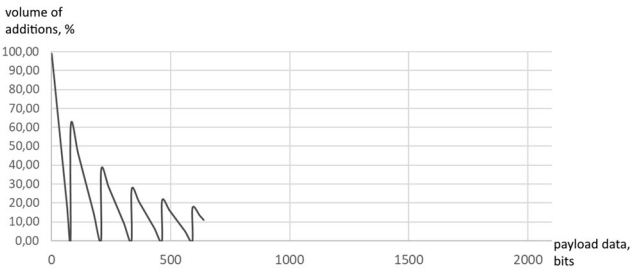

Figure 11. The volume of additions in the WirelessHART protocol

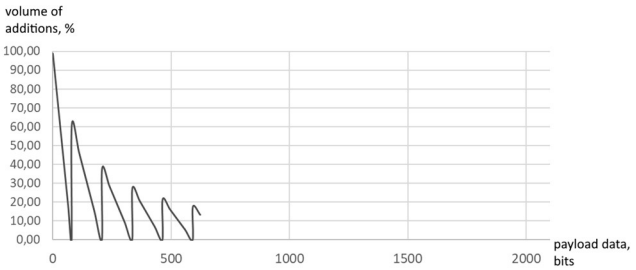

Figure 12. The volume of additions in the NB-IoT protocol

IV. RESULTS

The graphs show that as the payload volume increases, the impact of the addition on the total data packet decreases. When adding a lot of bits to create the encryption key's multiplicity, the peaks in the graph must be highlighted.

We also examined the average percentage of additions compared to the payload for each protocol and standard.

Table 2 shows that the more data a protocol or standard can transmit, the smaller the average percentage of additions a data packet will contain. However, modern IoT devices are energy efficient and transmit small amounts of data, so it is not reasonable to calculate the share of additions relative to the payload based on their maximum size

Table 2. Average percentage of additions

Protocol or standard	Average percentage of additions in encrypted data	Maximum payload size
Wi-Fi	2.13%	2304 bytes
Bluetooth	10.64%	251 bytes
6LoWPAN	23.22%	80 bytes
WirelessHART	23.08%	80 bytes
ZigBee	24.81%	68 bytes

NB-IoT	25.96%	65 bytes

Since the data in Table 1 represents averages of the maximum payload, it is inappropriate to use these values to assess the ultimate impact. To evaluate this impact, three distinct sets of payload data were generated.

The first set has the following structure:
path:34
value:170
The second set of data:
path:/module/send
value:170
The third set of data:
path:/module/send
value:option1

For each set, the payload size was calculated in bytes. Each character in the payload, including the line separator, consumes 1 byte. Therefore, the first set is 17 bytes, the second set is 27 bytes, and the third set is 30 bytes.

Using formula (1), the volume of additions for each protocol was calculated to achieve a multiple of the encryption key. The calculation results are shown in Table 3.

Table 3. Volumes of additions in packets for each protocol

Protocol or standard	Set 1	Set 2	Set 3
Wi-Fi	120 bits	40 bits	16 bits
Bluetooth	88 bits	8 bits	112 bits
ZigBee	96 bits	16 bits	120 bits
6LoWPAN	72 bits	120 bits	96 bits
WirelessHART	72 bits	120 bits	96 bits
NB-IoT	120 bits	40 bits	16 bits

The percentage of additions in the encrypted data was calculated using the volume of additions. The results are shown in Table 4.

Table 4. Percentage of additions in encrypted data

Protocol or standard	Set 1	Set 2	Set 3
Wi-Fi	46.68%	15.63%	6.25%
Bluetooth	39.29%	3.57%	31.82%
ZigBee	41.38%	6.90%	33.33%
6LoWPAN	34.62%	35.71%	28.57%
WirelessHART	34.62%	35.71%	28.57%
NB-IoT	22.92%	15.63%	6.25%

For each set, data packets according to the protocols were generated, and the volume of additions relative to the size of the whole data packet was calculated. The results are shown in Table 5.

Table 5. Percentage of additions in data packets

Protocol or standard	Set 1	Set 2	Set 3
Wi-Fi	22.73%	7.58%	3.03%
Bluetooth	28.95%	2.63%	25.93%
ZigBee	16.67%	2.78%	17.05%
6LoWPAN	18.37%	23.08%	18.46%
WirelessHART	16.36%	21.13%	16.90%
NB-IoT	38.46%	12.82%	5.13%

For each protocol, the average volume of additions in the packet is calculated according to the sets described earlier. The results are shown in Table 6.

Table 6. The average volume of additions in packets for the three sets of payload

Protocol or standard	Volume of additions
Wi-Fi	11.11%
Bluetooth	19.17%
ZigBee	12.16%
6LoWPAN	19.97%
WirelessHART	19.17%
NB-IoT	18.80%

Since the values obtained correspond to test datasets only, the average amount of additions in the range from 1 to 512 bits (64 bytes) of data was calculated. The calculation results are shown in Table 7.

Table 7. The average size of additions in packets with up to 64 bytes of payload

Protocol or standard	The average amount of additions
Wi-Fi	9.95%
Bluetooth	16.31%
6LoWPAN	11.55%
WirelessHART	10.12%
ZigBee	8.00%
NB-IoT	20.21%

The volume of additions has the most significant impact on the NB-IoT protocol. The Bluetooth standard follows it. The ZigBee protocol is the best performer, which may indicate that it is well-suited for systems with limited payload.

V. CONCLUSION

Modern IoT standards and protocols require data encryption. Since the encryption algorithms require the payload to be added to the key size, usually 128 bits, there is a problem of transmitting excessive information, which is, on average, about 26% of the payload in a packet. At the same time, the overall impact on traffic volumes in most protocols is about 10%, except for Bluetooth with 16% and NB-IoT with 20%.

To optimize traffic volumes, it is necessary to consider the size of the data in the packet, paying attention to the fact that not only is the payload encrypted, but also other parts.

The analysis of popular protocols regarding the percentage of "additional" information caused by the encryption showed that, from this point of view, the ZigBee protocol can be recommended for use in systems with a limited payload. However, when choosing a protocol in the design of an IoT system, the impact of encryption should be considered as one of many factors that will help in the final decision. Some other factors are discussed in [1], which can be extended by considering the impact of encryption by adding another coefficient to the Boolean functions of the protocol selection.

The paper presents a new quantitative assessment of the impact of encryption on traffic volumes in Internet of Things

(IoT) protocols. In contrast to previous works that have mainly focused on the energy consumption or computational costs of encryption, the study provides a detailed comparison of six widely used IoT communication protocols (Wi-Fi, Bluetooth, ZigBee, 6LoWPAN, WirelessHART, and NB-IoT) in terms of the transmission overhead caused by encryption. A mathematical model is developed, and an empirical evaluation is carried out using real data transmission scenarios to measure the volume of additional data caused by encryption. The study proposes a new selection criterion - encryption overhead - to improve decision-making when selecting protocols for IoT systems, complementing criteria such as delay, energy efficiency, and bandwidth.

References

[1] V. Kozel, O. Ivanchuk, I. Drozdova, O. Prykhodko, "Automation of the protocol selection process for IoT systems," *International Journal of Computing*, vol. 21, issue 2, pp. 251-257, 2022, https://doi.org/10.47839/ijc.21.2.2594.

[2] V. Kozel, O. Ivanchuk, I. Drozdova, O. Prykhodko, "Research of the methods for optimizing energy consumption in IEEE 802.15.4 protocols," *Scientific Notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences*, vol. 35(74), pp. 112-117, 2024, https://doi.org/10.47839/ijc.21.2.2594.

[3] O. Ivanchuk, "Research into methods for optimizing energy consumption in Internet of Things protocols," Bulletin of the Kherson National Technical University, vol. 4(91), pp. 273-279, 2024, https://doi.org/10.35546/kntu2078-4481.2024.4.35. (in Ukrainian)

[4] V. A. Memos, K. E. Psannis, "Encryption algorithm for efficient transmission of HEVC media," *Journal of Real-Time Image Processing*, vol. 12, pp. 473-482, 2016, https://doi.org/10.35546/kntu2078-4481.2024.4.35.

[5] V. K. Sarker, T. N. Gia, H. Tenhunen, T. Westerlund, "Lightweight security algorithms for resource-constrained IoT-based sensor nodes," *Proceedings of the IEEE International Conference on Communications (ICC)*, Dublin, pp. 1-7, 2020, https://doi.org/10.1109/ICC40277.2020.9149359.

[6] K. Kerpez, G. Ginis, J. Cioffi and S. Galli, "Virtualized broadband networking and standards in IEEE and broadband forum," *Proceedings of the 2014 IEEE Globecom Workshops (GC Wkshps)*, Austin, TX, USA, pp. 734-739, 2014, https://doi.org/10.1109/GLOCOMW.2014.7063520.

[7] R. Laufer, L. Kleinrock, "The Capacity of Wireless CSMA/CA Networks," *IEEE/ACM Transactions on Networking*, vol. 24, pp. 1518-1532, 2016, https://doi.org/10.1109/TNET.2015.2415465.

[8] Firdaus, E. Nugroho, A. Sahroni, "ZigBee and wifi network interface on wireless sensor networks," *Proceedings of the Makassar International Conference on Electrical Engineering and Informatics (MICEEI)*, 2014, pp. 54-58. https://doi.org/10.1109/MICEEI.2014.7067310.

[9] A. M. Alsahlany, Z. H. Alfatlawy, A. R. Almusawy, "Experimental evaluation of different penetration security levels in wireless local area network," *Journal of Communications*, vol. 13, no. 12, pp. 723-729, 2018, https://doi.org/10.12720/jcm.13.12.723-729.

[10] R. Velayutham, D. Manimegalai, "CCMP advanced encryption standard cipher for wireless local area network (IEEE 802.11i): A comparison with DES and RSA," *Journal of Computer Science*, vol. 11, pp. 283-290, 2015. https://doi.org/10.3844/jcssp.2015.283.290.

[11] I. Saberi, B. Shojaie, M. Salleh, M. Niknafskermani, "Enhanced AES-CCMP key structure in IEEE 802.11i," *Proceedings of the 2011 International Conference on Computer Science and Network Technology*, 2011, pp. 625-629. https://doi.org/10.1109/ICCSNT.2011.6182011.

[12] W. Indrasari, F. Sakinah, U. Umiatin, "Microplastic waste polluted water measurement development based on parameter of physics," *Journal of Physics: Conference Series*, vol. 2193, 2022. https://doi.org/10.1088/1742-6596/2193/1/012051.

[13] J. Tosi, F. Taffoni, M. Santacatterina, R. Sannino, D. Formica, "Performance evaluation of bluetooth low energy: A systematic review," *Sensors*, vol. 17, no. 12, p. 2898, 2017. https://doi.org/10.3390/s17122898.

[14] S. Yaniv, W. Avishai, "Cryptanalysis of the Bluetooth E0 cipher using OBDD's," *IACR Cryptology ePrint Archive*, vol. 72, pp. 187–202, 2006. https://doi.org/10.1007/11836810_14.

[15] "ZigBee Specification," *Davis, CA*, 2015, [Online]. Available at: https://lucidar.me/en/zigbee/files/docs-05-3474-21-0csg-zigbee-specification.pdf.

[16] A. Rizzardi, S. Sicari, A. Coen-Porisini, "Analysis on functionalities and security features of Internet of Things related protocols," *Wireless Networks*, vol. 28, pp. 2857-5887, 2022, https://doi.org/10.1007/s11276-022-02999-7.

[17] R. P. R. Pasala, R. N. Bhukya, "A comprehensive analysis of design and simulation of power optimized CRC algorithm for ZIGBEE application," vol. 6, pp. 127-134, 2017. https://doi.org/10.17577/IJERTV6IS040137.

[18] J. Higuera, J. Polo, "Understanding the IEEE 1451 standard in 6loWPAN sensor networks," *Proceedings of the 2010 IEEE Sensors Applications Symposium (SAS)*, Limerick, Ireland, 2010, pp. 189-193, https://doi.org/10.1109/SAS.2010.5439427.

[19] M. Tanveer, G. Abbas, Z. H. Abbas, M. Waqas, F. Muhammad, S. Kim, "S6AE: Securing 6LoWPAN using authenticated encryption scheme," *Sensors*, vol. 20, no. 9. p. 2707, 2020, https://doi.org/10.3390/s20092707.

[20] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig, "Securing communication in 6LoWPAN with compressed IPsec," *Proceedings of the International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, 2011, pp. 1-8, https://doi.org/10.1109/DCOSS.2011.5982177.

[21] C. Chan, G. Ee, C. K. Ng, F. Hashim, N. Noordin, "Development of 6LoWPAN adaptation layer with fragmentation and reassembly mechanisms by using Qualnet simulator," *Informatics Engineering and Information Science. ICIEIS 2011. Communications in Computer and Information Science*, Springer, Berlin, Heidelberg, vol. 254, 2011, pp. 199–212. https://doi.org/10.1007/978-3-642-25483-3_16.

[22] Y. Liu, R. Candell, K. Lee, N. Moayeri, "A simulation framework for industrial wireless networks and process control systems," *Proceedings of the IEEE World Conference on Factory Communication Systems (WFCS)*, 2016, pp. 1-11. https://doi.org/10.1109/WFCS.2016.7496495.

[23] I. Konovalov, "A framework for WirelessHART simulation," *SICS Technical Report*, Kista, vol. 6, pp. 1-39, 2010.

[24] S. Raza, A. Slabbert, T. Voigt, K. Landernäs, "Security considerations for the WirelessHART protocol," *Proceedings of the IEEE Conference on Emerging Technologies & Factory Automation*, 2009, pp. 1-8. https://doi.org/10.1109/ETFA.2009.5347043.

[25] S. Hessel, D. Szczesny, N. Lohmann, A. Bilgic, J. Hausner, "Implementation and benchmarking of hardware accelerators for ciphering in LTE terminals," *Proceedings of the 2009 IEEE Global Telecommunications Conference GLOBECOM'2009*, Honolulu, HI, 2009, pp. 1-7. https://doi.org/10.1109/GLOCOM.2009.5426313.

[26] G. Zhao, H. Chen, J. Wang, "A lightweight block encryption algorithm for narrowband Internet of Thing," *Peer-to-Peer Networking and Applications*, vol. 16, pp. 2775-2793, 2023. https://doi.org/10.1007/s12083-023-01559-w.

[27] A. D. Dwivedi, G. Srivastava, "Differential cryptanalysis in ARX ciphers with specific applications to LEA," *Cryptology ePrint Archive*, vol. 2018, issue 898, 2018. [Online]. Available at: https://eprint.iacr.org/2018/898.pdf.

***VIKTOR KOZEL**, PhD in Engineering Sciences (2017), Master in Computer Engineering, Kherson National Technical Uinversity (2020). Current position: an Associate Professor of the Department of Computer Systems and Networks of Kherson National Technical University, Ukraine. Scientific interests: networks, IoT, control systems.*

***OLEKSII IVANCHUK,** Master in Computer Engineering, Kherson National Technical University (2020). Current position: a postgraduate student of the Department of Computer Systems and Networks of Kherson National Technical University, Ukraine. Scientific interests: sensor networks, IoT, energy optimization, WEB-development, cloud systems.*

***IEVGENIIA DROZDOVA** graduated from Kyiv Polytechnic Institute, the speciality of Automated Control Systems, qualification of System Engineer (1986). Current position: a Senior Lecturer of the Department of Computer Systems and Networks of Kherson National Technical University, Ukraine. Scientific interests: programming, databases, IoT.*

***OLENA PRYKHODKO** graduated from Kherson State Pedagogical Institute, the speciality of English and German Languages (1999). Current position: a Senior Teacher of the Department of Foreign Languages of Kherson National Technical University. Ukraine. Scientific interests: modern technologies for teaching foreign languages, the use of multimedia technologies in the educational process English for specific purposes.*